Security +

Threat Classifications

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

Types of Threat Actors

- Hactivist
- Script Kiddies
- Insiders
- Competitors
- Organized Crime
- Nation State
- APT (Advanced Persistent Threats)
- Grey Security Companies

White-hat

- Attacker who is legally penetration testing a network or organization

Grey-hat

- Attacker who may use some illegal methods while penetration / compromising a network or organization and uses that information to coerce organizations to pay for that information
- Also attackers who may have good intentions but cross legal boundaries

Black-hat

- Attacker who uses illegal methods to penetrate systems and gains from the penetration such as by using the network resources or reputation on the dark-web

Bots and Botnets

- Bot means robot, net means network
- Can be embedded systems such as routers, printers, IoT, and the like
- Can effectively perform DDOS attacks
- Can perform recon against a wide array of publicly accessible services

Types of Attacks

Privilege escalation

- Attempt to gain access privilege at a higher level than the user has been assigned by the security administration

Application / Services attacks

- Attacks on a particular IP/ port / protocol combination of a running network service

Network stack attacks

- IP spoofing / MAC spoofing / ARP poisoning

Hash based attacks

Replay attacks

- Sensitive data can be captured and re-used such as authentication credentials
- Examples include physical access tokens, PPP / CHAP network authentication attacks, WEP authentication attacks

Steps of Malware Operation

1. **Infection -** Get onto the target machine by vector (USB, malvertising, spyware, drive-by-download, malware, web-vulnerability, buffer-overflow, etc)
2. **Search -** Map and scan the available network
3. **Update -** Download updates relative to the scan results
4. **Compromise -** Attempt to compromise the other nodes on the network
5. **Control -** Implement malicious changes to the newly compromised systems
6. **Deceive and Destroy -** Alter logs to hide from monitoring systems

Vulnerability Factors

- Confidentiality Impact
- Integrity Impact
- Availability Impact
- Gain Access Impact
- Privilege Escalation Impact
- Remote or Physical Access Required
- Complexity Required
- Published or Not

Malware Types

Worms

- Attempts to pivot to other network devices after infecting the first device

Logic Bombs

- Executes in response to other events
- The malware will not execute for a week after infection to hide the source of attack, or it will only operate at night when the victim is not at the computer, etc.

Trojans

- Uses a software application (or extension) installation to infect a host
- Some other terms are **rogueware** and **scareware**

Ransomware

- Attempts to take a victims system or data hostage and extract payment to restore functionality or data

Rootkits

- Attempts to gain root level access to the system in order to hide it's tracks
- Installs lower level services that can be more difficult to detect such as in the BIOS, boot sector, at the kernel level, or hardware level
- Typically intercept and modify the operating system's APIs
- Some examples from the media include Sony BMG copy-protection rootkit scandal, and Stuxnet programmable logic controller **(PLC)** rootkit
- Can be very difficult or even impossible to get rid of when the rootkit gains persistent hardware corruption
- Types include:
  - User mode
  - Kernel mode
  - Boot level
  - Hypervisor level
  - Firmware / Hardware mode

Spyware

- Remote monitoring software that can log user activity or exfiltrate files
- Also can be advertisements that collect and build user metrics on a particular user for use in targeting social networking scams or social engineering, or spam

RAT Remote Access Trojan

- Malware that allows attackers to take control of systems from remote locations

Adware

- Used to build user profiles to target users with ads and scams

Keylogger

- Records and exfiltrates users keystrokes to attempt to steal information such as passwords and usernames

Armoured Virus

- Designed to hide the signature of the virus behind code that confuses or blocks the antivirus software from detection
- Designed to be very difficult to reverse engineer and analyze
- Overly large, because it contains a large amount of misleading logic in order to foil attempts to figure out its mission

Polymorphic Virus

- Complicated computer virus that affects data types and functions
- It is a **self-encrypted** virus designed to **avoid detection** by a scanner
- Upon infection, the polymorphic virus **duplicates** itself by creating usable, albeit **slightly modified** copies of itself

Stealth Virus

- **Hidden** computer virus that attacks operating system processes and **averts typical anti-virus** or anti-malware scans
- Stealth viruses **hide in files**, **partitions and boot sectors** and are adept at **deliberately avoiding detection**

Retroviruses / Anti-antivirus

- Attempt to render your antivirus software unusable and leave you exposed to other less formidable viruses

Social Engineering Attack Types

- **Flattery, conning, etc.**
- **Posing as authority**
- **Encourage someone to do something risky**
- **Impersonate someone**
- **Tailgating**
- **Shoulder surfing**
- **Hoax**
- **Dumpster diving**
- **Watering hole attack**
  - Going to a popular bar, restaurant, coffeeshop, or other social
- **Spam**
  - Unwanted email form a legitimate sender of the email, usually as part of a marketing campaign and / or to maintain engagement with their products
- **Phishing**
  - Tricking users into clicking on links that send them to malicious websites, install malware, or revealing malicious PII
  - Phishing can also be used to validate an email is legitimate by including beacon or ping-back links in images
  - Also, phone scams are phishing attacks
- **Spear-phishing**
  - A phishing attack that targets a single user or smaller group of users explicitly
- **Whaling**
  - Social engineering attacks that go after executive level or other people in power positions
- **Vishing**
  - A VOIP phishing attack
- **Psychology of Social Engineering**
  - **Authority**
    - Take advantage of the reaction people have to fear of not doing what their boss would want

    - **Intimidation**
        - Intimidate is similar to fear of authority, but can just be physical intimidation, or annoying
    - **Consensus**
        - Fake testimonials, group think, network effects
    - **Scarcity**
        - Creating an image that something is rare or will be out of stock soon
    - **Urgency**
        - Create a timer that scares people into doing something
    - **Familiarity**
        - Imitating common websites such as Google, PayPal, etc., or foundations or companies related to your company
    - **Trust**
        - Building trust with someone first then exploiting the victim

Wireless Attacks

Disassociation Attack

- Removes a wireless client from a wireless network
- Can prevent users (DOS) from connecting to a specific wireless network
- Sends a disconnection request to the AP with a spoofed MAC address of the victim
- Management frames of WEP are not encrypted so, disconnection frames are easily spoofed with a clients MAC address
- **WPA2 management frames** are **unencrypted** and **WPA3 management frames** are required to be **encrypted** using a **group temporal key** which mitigates the authentication attack

Rouge AP

- A **malicious unauthorized AP** in a location that allows users to connect
- Victims connect to the unauthorized AP instead and attackers can exfiltrate communications
- Also, a rouge AP can be plugged into piece of hardware such as a switch and hidden from sight
- The attacker can then access the internal network from the AP

Evil Twin

- A rouge access point with the **same SSID as a legitimate AP**
- The devices will connect to the malicious AP if the signal strength is higher than the legitimate AP

Jamming Attack

- Transmit a **disruptive radio signal** on the same frequency as the wireless network
- This interferes with the wireless transmission and can seriously degrade performance
- This can be used as a disassociation attack

IV attacks (Initialization vector attack)

- Attempts to discover the **pre-shared key** from the **IV**
- The **IV** is **passed with the cipher text** in **802.11 WEP**
- The **IV** is **only 24 bits long** so relatively easy to brute force
- Once an attacker learns the plaintext of one packet, the attacker can compute the RC4 **key-stream** generated by the **IV** used

NFC Attack (near field communications attack)

- During an NFC attack passively monitors and captures traffic between two other NFC devices

Bluetooth Attacks

- Within short range (about 3 meters) wireless system used for PAN (personal area networks)
- **bluejacking**
  - **Sending unsolicited messages** such as text, images and sounds
- **bluesnarfing**
  - Tools (such as **hcitool and obexftp**)
  - **Exfiltrating data** such as email, files
- **bluebugging**
  - Is more extensive remote access and logic bomb access

Wireless Replay Attacks

- Passively captures data between two devices, modifies it and then attempts to **impersonate the client or server**, by using the captured data to identify and authenticate
- WPA2 using CCMP (which uses AES) is currently not vulnerable to replay attacks
- **WEP and WPA** using **TKIP** are vulnerable to **replay attacks**

RFID Attacks (Radio Frequency Identification)

- **Sniffing or eavesdropping** within range if the radio frequency is known
- Replay attacks are possible
- DOS by jamming the radio frequency with noisy signal / spray

SMS Short Message Service and MMS Multimedia Messaging Service

- Attacker tricks the recipient into **visiting a malicious** website or into doing something else that **executes malicious files**
- Vulnerabilities in a core Android component called **Stagefright** that is used to process, play, and record multimedia files
- In some cases doesn’t require any interaction from the user; the phone just needs to receive a malicious message

Generic Types of Attack

DOS Denial of Service Attacks

- **DOS** attacks attempt to disrupt availability of an online service

- **DDOS** is an attack from (or seeming to come from) more than one computer against a single target

Masquerade attack

- Any attack where an attacker has gained knowledge of a legitimate username and password, or is able to trick an authentication process by spoofing an IP address or MAC address

Amplification attacks

- Uses a method to increase the amount of traffic being sent to or requested from a victim

MITM Man in the middle Attacks

- Can be performed by a device in the network path and **allows interception of traffic or eavesdropping**
- Can allow **malicious modification of DNS resolution** and send attackers to malicious imitation sites
- If a browser's **trusted certificate store** can be altered, MiTM can act as a **transparent TLS proxy** and pick off credentials and modify a connection's data in transit
- APR cache can be changed

ARP Poisoning Attacks

- **ARP request** broadcasts a request for a machine with a particular IP address to respond with its MAC address
- **ARP Reply** the device with the IP address of the request replies with it's MAC address
- ARP is very trusting - it will generally believe any reply packet
- ARP Poisoning can result in MITM and DOS attacks

DNS Attacks

- **DNS Poisoning attack**
- **DDOS DNS attacks**
- **Pharming Attack** modifies the clients DNS hosts file in order to reroute the victim to malicious IP address instead of the legitimate server
- **DNS Amplification attacks**
- Attempts to confuse legitimate DNS servers by sending malformed / source spoofed DNS queries in some way to amplify a normal DNS query

Brute Force Attacks

- Attempts to guess all the possible character combinations
- Possible to implement this attack **online** and **offline**

Dictionary Attacks

- Standard dictionary attack uses words int he dictionary or another prepared list of words to try in combination with numbers
- Rainbow table attacks use a database or file containing all the hashes prepared for a prepared set list of common password combinations

- If a hacker is able to steal the password database from a website or server, then the rainbow table can be used to see if any common passwords in the stolen database of password hashes match the rainbow table entries

Replay Attacks

- Reuses data that was intercepted from a previous communication to impersonate a user or device
- Can be used agains wired or wireless networks

Pass-the-hash attack

- When an attacker has attained the hash of a user's password through network sniffing and can replay that hash to the network authentication service such as NTLM or LANMAN protocols.
- These are mitigated with modern authentication suites

Plaintext attacks

- If the attacker knows the plaintext of the encrypted data and has a copy of both plaintext and encrypted data
- Use both sets of data to determine the encrypted method and key, IV, etc.

Typo Squatting / URL Hijacking

- But a domain that looks similar to a legitimate domain name
- Possible to take advantage of spelling mistakes or language sets of unicode character set
- Also possible to buy a domain name and put a well-known domain as a sub-domain
- The benefits of this type of hijacking includes: earning money from ads, malicious websites that attempt to hack clients browsers, reselling the domain

Homograph / Punycode Attacks

- Attack that leverages some browsers (but not all) **conversion of other language character sets into ASCII**
- Punycode is type of encoding used by browsers that converts the international domain-name systems which only allows limited character set (A-Z, a-z, 1-9, and "-") into unicode for the url bar
- Registering a domain using punycode can make the url look identical to another domain

Clickjacking

- Tricks users into clicking something that is different than what they think they are clicking on
- Masking a url link with an href that points to a different location

Session Hijacking

- Accesses a browsers session ID stored in cookies
- Can be used in a replay attack if the server still has that cookie in a logged in state

Domain Hijacking

- Attacker changes the registration of a domain without permission from the owner

Man-in-the-browser

- Proxy trojan that can infect vulnerable browsers with malicious browser extensions
- It can capture keystrokes, session data

Driver Manipulation

- **Driver signing**
  - Ensures that the correct driver is being used / installed and that updates are authentic
- **Refactoring**
  - Is to **alter the code of the original driver** to make it more performance efficient or feature rich
  - Refactoring can also refer to **hacked drivers** such as a printer driver that send documents to a remote server
- **Shimming**
  - Is code that can be **run instead of the original driver**, the operating system intercepts the call to the original driver and redirects the call to the shimmed driver
  - More common than refactoring since driver signing can make that task very difficult

Zero Day Vulnerability Exploitation

- Weakness or bug that is unknown to the public and IT security community

Memory Leak Vulnerabilities

- Is a bug in a computer program that allows an **application** or **service** to use up all available memory resulting in resource exhaustionn

Integer Overflow Attacks

- Attempts to use or create **numerical values** that are **too large** for an application to handle

Buffer Overflow Attacks

- Occurs when application **receives more** input than it **expects**
- If the input is attempted to be written to memory, it will overflow the reserved memory space for that piece of information
- If the write overflow is able to **write system commands** into an adjacent part of memory that is marked as **executable memory** and would otherwise contain commands queued for execution, the attacker can achieve **arbitrary code execution**

Pointer Dereferencing

- Programming languages use pointers which are a reference to another memory location that contains data such as a variable (pointee)
- Pointers are also called references
- Dereferencing is the process of using the pointer to access the data
- If the dereferencing operation is a pointer that references a non-existent pointee it can cause the application to crash

Command Injection Attacks

- Occurs when user input includes operating system commands that are able to be evaluated and run

Cross-site scripting / XSS attacks

- Embedding html or javascript code into a website by including it in your comments or other input, getting in stored into the website's database or file and then having the code run on another user's browser when they visit the website
- Can capture session ID cookies, attack routers
- OWASP includes 10 rules that developers can follow to prevent XSS attacks
- Types of XSS include (https://owasp.org/www-community/Types_of_Cross-Site_Scripting):
  - **Persistent**
    - Is when user input is stored on a server, and then output to a webpage in such as way that allows the script to execute
  - **Reflected XSS**
    - Is when user input into a website can be immediately included into the resulting page script without being stored in the server database, such as search input boxes etc.
  - **DOM based**
    - When the entire XSS occurs within a single webpage DOM
- See: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Cookie Attacks

- Malicious websites can try to steal cookies that are stored on the user's computer by other websites
- These cookies may be **session cookies** which store session information for the user's logged in session, or other sensitive data such as credit card information, etc.
- A **zombie cookie** is a cookie that is able to escape the cookie storage memory

Header manipulation

- Manipulating headers can attempt to inject commands for the server or client to execute, or allow attackers to carry out other types of attacks such as cross-site-scripting, session-hijacking, cookie-stealing, and injection attacks
- Server's can be configured to either sanitize or ignore client-side sent

headers

Cross-site Request Forgery XSRF or CSRF (MORE!!!)

- Attacker tries get the victim to perform an action on a website without their knowledge
- Link-baiting / clickjacking
- Can attempt to set passwords or account email addresses on other accounts if the other site allows
- Form-tokens can help prevent XSRF against your site

DLL (Dynamic Link Library) Injection

- Injects a DLL into a system’s memory and causes it to run
- DLLs are compiled set of code that applications can access without having to include separate modules

LDAP Injection

- Uses **X.500 directory services** standard to **provide directory information**
- LDAP injections attacks include LDAP query commands into the web-request to retrieve unauthorized information such as system usernames, or directory structure

Directory traversal

- Attacks a web-server to **map directory structure** and **access unauthorized** files
- Proper web-server configuration and user input sanitization can mitigate this type of attack
- Using non-standard locations of resources can mitigate the ability of malware to traverse directories of common applications

XML Injection

- Extensible markup language sends malicious XML content to a web-application
- **Web-applications** need to be hardened against these types of attacks

Volume Based Attacks

- Includes UDP floods, ICMP floods, and other spoofed-packet floods
- The attack’s goal is to saturate the bandwidth or exhaust other hardware resources of the attacked site, and magnitude is **measured in bits per second (Bps)**

Protocol Attacks

- Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more
- This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is **measured in packets per second (Pps)**

Application Layer Attacks

- Includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or OpenBSD vulnerabilities and more
- Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in requests per second (Rps)

Teardrop Attacks

- A teardrop attack involves the hacker sending broken and disorganized IP fragments with overlapping, over-sized payloads to the victim's machine
- The intention is to crash operating systems and servers due to a bug in the way TCP/IP fragmentation is re-assembled
- Operating systems and many types of servers are vulnerable to this type of DOS attack, including Linux

DHCP Starvation Attacks

- Works by broadcasting DHCP requests with spoofed MAC addresses
- Easily achieved with attack tools such as **The Gobbler**
- Attackers can then set up a rogue DHCP server on their system and respond to new DHCP requests from clients on the network

Malvertising

- **Criminally controlled advertisements** embedded in websites track users activity **across multiple websites**
- Can also attempt to install malware on user's computers by **offering free software** such as software that **claims to** improve performance, or **hoaxing** the user into thinking that their computer is already infected and needs to be cleaned

Web-Server Attacks

Syn Flood Attacks

- sending multiple SYN packets but never completes third part of the TCP connections by sending the last ACK packet

Slow loris / Low-rate Denial-of-Service attacks

- The Low-rate DoS (LDoS) attack is designed to exploit TCP's slow-time-scale dynamics of being able to execute the retransmission time-out (RTO) mechanism to reduce TCP throughput
- In short, a hacker can create a TCP overflow by repeatedly entering a RTO state through sending high-rate and intensive bursts – whilst at slow RTO time-scales
- The TCP throughput at the victim node will be drastically reduced while the hacker will have low average rate thus making it difficult to be detected

Internet Control Message Protocol (ICMP) flood

- Internet Control Message Protocol (ICMP) is a connectionless protocol used for IP operations, diagnostics, and errors

- An ICMP Flood – the sending of an abnormally large number of ICMP packets of any type (especially network latency testing "ping" packets)
- Can overwhelm a target server that attempts to process every incoming ICMP request, and this can result in a denial-of-service condition for the target server

Peer-to-peer attacks

- A peer-to-peer (P2P) network is a distributed network in which individual nodes in the network (called "peers")
- Peers act as both suppliers (seeds) and consumers (leeches) of resources, in contrast to the centralized client-server model where the client-server or operating system nodes request access to resources provided by central servers

War-driving

- Driving around looking for open wireless networks for the purpose of accessing the Internet
- The attacker may also be able to accomplish other types of attacks on the network such as:
- Passing monitoring of cleartext communication on an open network
- Mapping networks if open WiFi networks also multi-cast network information
- Results can then be uploaded to websites like WiGLE, openBmap or Geomena where the data is processed to form maps of the network neighbourhood

War-dialing

- A technique to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for modems, computers, bulletin board systems (computer servers) and fax machines